STATE OF HAWAIʻI
INFORMATION PRIVACY AND SECURITY COUNCIL

Category	Security	Title	**Multi-Function Copier/Printer**
Document:	IPSC2010-03	Revision:	**2010.07.19 DRAFT**
Posted URL:	http://ipsc.hawaii.gov		
Status Under Review		Revised on:	July 19, 2010
Authority:	State of Hawaiʻi IPSC	Exceptions:	Temporary Allowed
Applicability	☒ State Government Agencies ☒ All ..... Guideline ☐ Excluding: None ..... Not Applicable ☐ Including: None ..... Not Applicable ☒ State Funded Entities ..... Guideline ☒ Other: County Government Agencies & Attached ..... Guideline		

I. I. PURPOSE

Technology has increased the demand for more paperless operations, which has increased the need for scanning capability in many operational processes and communication protocols. Counties and State of Hawaii departments and agencies, must rely on digital scanners that will be appropriate to meeting increasing administrative needs. The purpose of this document is to provide basic guidelines for all State and County agencies for protection of sensitive information on digital scanners.

II. SCOPE

These guidelines are provided to all Chief Financial Officers of each State and County government agency whose employees in their office of procurement and contracts have the responsibility to communicate appropriate purchasing guidelines for digital scanners.

This guideline meets only the requirements imposed by the State of Hawaii. Agencies/Departments that work with federal information of a confidential or sensitive nature must also ensure that digital scanners are in compliance with all federal requirements.

III. TERMS AND DEFINITIONS

Personal Information - As defined in Act 135 and Act 136, Session Laws of Hawaii 206, an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number;
2. Driver's License number or Hawaii identification card nmber; or
3. Account number: credit or debit card number, access code, or password that would permit access to an individual's financial account. (Note: Includes pCard/credit cards issued to employees for agency purchase purposes)

Sensitive Information – Any type of information such that the loss, misuse, or unauthorized access to or modification of could adversely affect the Counties and State of Hawaii departments and agencies. Personal information as defined above are considered to be a subset of "Sensitive Information". Examples of sensitive information include information protected by other regulations such as HIPAA and FERPA.

Encryption – Transformation of information into a form that cannot be read or interpreted by others without knowledge of how it was transformed. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Data Overwrite – An option on a digital scanner to overwrite the sector of the hard drive used for data processing either after the completion of each job, or on demand from the devices console.

Hard Drive Surrender – This is a service performed by a vendor. This service option allows an authorized technician to remove the hard drive from the digital scanner and provide the customer custody of the hard drive.

IV. POLICY

All State and County government agency employees are responsible for the safekeeping of information read by a digital scanner.

All State and County government agency employees must provide immediate notification to their respective agencies and/or supervisors following the loss of any agency-owned digital scanner and/or hard drive of any agency-owned digital scanner.

Appropriate and timely action must be taken if Sensitive and/or Personal Information are contained on the lost or stolen hard drive of a digital scanner in accordance with the Agency's Policies and Procedures.

V. STANDARDS

Use of digital scanners are increasing in County and State agencies allowing employees the advantage of quicker turnaround for tasks requiring multiple hard copies of an original document, as well as to convert a hard copy of a document to a soft/electronic copy for the purpose of viewing documents electronically. While increasing productivity, use of these devices without taking the proper security

1. Digital scanners installed on workplace networks must be configured to allow only controlled access:
    a. Scanned to network folders must be configured on internal workplace local area networks, allowing access to only authorized personnel.
    b. Scanned to email accounts must be limited to only authorized personnel.
    c. Wireless access to digital scanners must be configured on internal workplace local area networks, allowing access to only authorized personnel.
    d. Allowances for external remote access must be configured to specific individuals, and such individuals shall be allowed access only after request to authorize, is approved by the workplace network administrator.

2. Use of Encryption:
    a. Digital scanners with documents saved to the scanner's hard drive must store files using encryption.
    b. External remote access to the digital scanner must be configured with username and password, and external access must be through an encrypted web access, to block intruders tapping the network.

3. Data overwrite:
    a. Digital scanners with hard drives must be configured to either data overwrite data after every scan, or allow the user to invoke data overwrite from the scanner's console.

4. Physical security:
    a. Do not leave digital scanners unattended for even a short while.
    b. Limit use of the digital scanner to only to authorized personnel.

5. Disposal and End of Lease Return:
    a. Before disposing digital scanners equipped with hard drives, information on the hard drive must be removed by either invoking data overwrite, or removal of the hard drive.
    b. Leased digital scanners equipped with hard drives, must have the information on the hard drive removed by either invoking the data overwrite, or invoking the hard drive surrender option.
    c.

VI. COMMENTS AND SUGGESTIONS

Comments, recommendations, proposals, or suggestions regarding the contents of this document may be sent via email to:

IPSC@hawaii.gov

or in writing to:

Information Privacy and Security Council
c/o Information and Communication Services Division
1151 Punchbowl Street, Room B10
Honolulu, HI 96813

VII. REVISION HISTORY

Creation Date:	Date Last Updated	Date last reviewed
July 19, 2010	July 19, 2010	July 19, 2010

Revision History		
Revision date	**Revision**	**Author**
July 19, 2010	First Draft	Information Privacy & Security Council

_____ _____

Russ K. Saito, Chairperson Date
Information Privacy and Security Council